ABSTRACT

The development of Software Defined Network increases network management flexibility by separating the control plane and data plane, but it is vulnerable to SNMP Amplification-based Distributed Denial of Service attacks that flood SNMP ports (161) with UDP packets. This research develops a detection and mitigation system using Support Vector Machine for detection and Access Control List for mitigation in SDN. Simulations were conducted using Mininet and Ryu Controller on a topology with two switches and ten IP hosts (10.0.0.1–10.0.0.10). Traffic data was collected via Traffic_Logger.py, generating features such as packet count, packet rate, and average packet size, processed using Pandas and NumPy. The Support Vector Machine model with an RBF kernel was trained using 70% training data and 30% testing data, detecting attacks based on feature thresholds. ACLs were dynamically applied via the Ryu Controller and iptables. Testing included normal, attack, and mitigation scenarios. Results show SVM accuracy >90% and effective Access Control List mitigation in restoring network performance. Results also show a reduction in packet loss from 20% to 2% after mitigation, indicating that ACL is effective in mitigating SNMP Amplification attacks. Real-time visualization via Matplotlib facilitates monitoring. This research contributes to Software Defined Network security, though limited to simulation.

Keywords—***Software Defined Network, Distributed Denial of Service, SNMP Amplification, Support Vector Machine, Access Control List, Mininet, Ryu Controller.***